Department of the Army **FORSCOM Memorandum 25-2**
Headquarters, United States Army Forces Command
1777 Hardee Avenue, SW
Fort McPherson, Georgia 30330-1062
31 May 2005

Information Management
Information Assurance

History. This publication is a new Forces Command (FORSCOM) memorandum.
Applicability. This memorandum (regulation) applies to Headquarters, Forces Command staff agencies and all organizations, units, and activities utilizing the FORSCOM Command and Control System Networks.
Changes. Changes to this memorandum are not official unless they are authenticated by the HQ FORSCOM, Deputy Chief of Staff, G-6 (DCS, G-6 or G-6).
Suggested Improvements. The proponent for this memorandum is the G-6. Users are invited to send comments and suggested changes on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Commander, HQ FORSCOM, DCS, G-6 (AFCI-IC), 1777 Hardee Avenue, SW, Fort McPherson, GA 30330-1062

FOR THE COMMANDER:

OFFICIAL:

DAVID D. McKIERNAN
Lieutenant General, USA
Deputy Commanding General/
Chief of Staff

//SIGNED//
WILLIAM T. LASHER
Colonel, GS
Deputy Chief of Staff, G-6

DISTRIBUTION: This memorandum is intended for all Fort McPherson and Fort Gillem operating activities.

Copy Furnished: CDR, Fort McPherson (IMSE-MPH-HRS) (record copy)

TABLE OF CONTENTS

SECTION I
General

1-1. Purpose.

The purpose of the memorandum is to provide policy and best business practices to protect information systems and safeguard information contained in the Forces Command (FORSCOM) Command and Control System (FCCS) Networks from unauthorized or inadvertent modification, disclosure, destruction, denial of service and use.

1-2. References.

a. Department of Defense 5500.7-R, Joint Ethics Regulation (JER), 30 August 1993.

b. Department of Defense (DOD) Instruction 5200.4, DOD Information Technology Security Certification and Accreditation (C&A) Process (DITSCAP), 30 December 1997.

c. Army Regulation 380-67, The Department of the Army Personnel Security Program, 9 September 1988.

d. Department of Defense Directive 8500.1, Information Assurance, 24 October 2002.

e. Department of Defense Instruction 8500.2, Information Assurance Implementation, 6 February 2003.

f. Army Regulation 25-2, Information Assurance, 14 November 2003.

g. FORSCOM Memorandum 380-5, Department of the Army Information Security Program, 15 November 2003.

h. Army Regulation 25-1, Army Knowledge Management and Information Technology Management, 30 June 2004.

1-3. Responsibilities.

a. Chiefs, directors and supervisors at all levels shall ensure that subordinate personnel are aware of their individual responsibilities to protect and use information systems installed on the FCCS networks in an authorized and effective manner.

b. The FORSCOM Designated Approving Authority (DAA) will:

(1) Ensure an effective Information Assurance (IA) Program is implemented.

(2) Assign written security responsibilities to the IA Program Manager (IAPM), IA Manager (IAM), IA Network Manager (IANM) and the IA Security Officer (IASO).

(3) Ensure all networks and information systems are certified and accredited in accordance with DOD Information Technology Security Certification and Accreditation Process.

c. The IAPM, IAM, IANM and IASO will:

(1) Have oversight and execute the IA program.

(2) Complete the required IA training as per AR 25-2.

(3) Ensure initial and annual IA awareness user training is conducted and documented.

(4) Ensure all passwords are maintained and controlled within the guidelines of this memorandum and Army directives.

(5) Ensure mandatory DOD anti-virus software and updates are loaded, operational and current.

(6) Report IA incidents to the Regional Computer Emergency Response Team (RCERT), as appropriate.

d. The System Administrators (SA) will:

(1) Install, configure, operate, and maintain the FCCS networks.

(2) Ensure the network configuration is in accordance with (IAW) the FCCS Computer Security Baseline.

(3) Enforce appropriate user permissions.

(4) Enforce the password policy as stated in this memorandum.

(5) Install all applicable Information Assurance Vulnerability Alerts (IAVAs) and updates to the network.

(6) Scan and report threats of the network to the IAM.

e. Automated Information System (AIS) user will:

(1) Complete the IA awareness training and successfully pass the IA awareness test.

(2) Use passwords or other FCCS provided access control measures.

(3) Check disks for viruses prior to use.

(4) Report suspected intrusions, viruses and unexplained operating anomalies to the FCCS Help Desk.

(5) Use government information systems for "official" business only, or as allowed in the JER and Acceptable Use Policy.

SECTION II
Information Assurance Policies and Best Business Practices

2-1. Acceptable Use Policy.

a. Access to the FCCS Secret Internet Protocol Router Network (SIPRNET), FCCS Nonclassified Internet Protocol Router Network (NIPRNET), and the Global Command and Control System (GCCS) Network is for official use and authorized purposes.

b. The FCCS Acceptable Use Policy defines the responsibilities of individual account holders to safeguard information contained in the FCCS SIPRNET, FCCS NIPRNET and GCCS from unauthorized or inadvertent modification, disclosure, destruction, denial of service and use.

c. All FCCS account holders are required to read and sign the Acceptable Use Policy at Appendix A.

d. The SAs have elevated rights and privileges allowing complete access and authority to the system to which they administer. The SA Acceptable Use Policy at Appendix B provides guidelines for SA rights.

2-2. Password.

a. Technical controls, particularly password authentication, must be adopted to ensure that access to information resources is limited to authorized personnel. Some of the more common uses for password include user level accounts, web accounts, e-mail accounts, screen saver protection, voice mail password, and local router logins. Thus, users must select strong passwords for their official and personal accounts.

b. Authentication: Authentication verifies the identity of a user of the FCCS network. Password is the most common authenticator for a user to access the FCCS network.

c. Passwords: Passwords will have a minimum of ten (10) case-sensitive characters. Passwords will be a mix of uppercase letters, lowercase letters, numbers and special characters, including at least two of each of the four types of characters that the user generates. The AIS will be configured to force compliance with this composition rule. Passwords will not include such references as social security numbers, birthdays, user identifications (IDs), names, slang, military acronyms, call signs, dictionary words, consecutive or repetitive characters, system identification, or anything easily guessed. There may be exceptions to password policy for some information systems. Specifically, the following policy applies to the password for information systems below:

(1) The GCCS JOBES Permission (JPERMS) password will consist of at least an eight (8)-character password (six (6) alpha and two (2) numeric). GCCS JPERMS generated passwords must be created in "lower case" only. The first character must be an alpha character. Special software is used to generate the user's initial password.

(2) A Blackberry device should have a five (5)-character, user-generated, alphanumeric password with a minimum of one (1) alpha and one (1) numeric. This criteria is IAW memorandum, DA CIO/G-6, (NETC-EST-A), 8 July 2004, subject: Password Protection for Two-Way Wireless E-mail Devices.

d. Initial System Passwords: Many systems come from the vendor with a number of standard user ID (e.g., system, test, administrator, etc.) already enrolled in the system. The SA will change all default vendor-supplied passwords for all user ID before connecting the AIS to the network or allowing the general user population to access the system.

e. Initial Password Assignment: The SA or IASO is responsible for generating and assigning the initial password for each user ID. The user will then be informed of this password. Upon initial login, the user will be required to immediately change the password. The GCCS Functional Manager is responsible for generating and assigning the initial password for each GCCS user ID. The user will then be informed of password. Upon initial login, the user will be required to immediately change the password, using JPERMS. Paragraph: 2-2, c, (1).

f. Password Change Authorization: The SA or IASO shall be permitted to change the password of any user at any time if he/she suspects any breaches in security. The SA or IASO will inform the user, responsible Information Management Officer (IMO) and IAM in such circumstances, but is not required to do so prior to the change. In the event of a security breach, the user will call his/her SA or IASO, who will set a new password as done with initial password assignment.

g. Domain Administrator Password: The Domain Administrator account password will be tightly controlled and issued by signature only from the IASO. The Command and Control Support Division, Network Services Branch Chief must approve access to this account password. Further, any additions to the Domain Administrators group must be approved by name.

h. Group Identification (ID): Based on needs and privileges to be assigned, group ID may be used to allow classification of users. However, there shall be no user ID used by more than one person to access data, thus circumventing individual user accountability. Establishing generic "temp", "guest" or other similar accounts for use by multiple or temporary users is strictly prohibited.

i. Account Deactivation and Deletion: User accounts will be deactivated immediately by the SA or IASO upon notification of an individual's voluntary or involuntary termination of employment, transfer, retirement, suspension of access to classified information, or revocation of security clearance. The supporting IMO will be notified of the account deactivation. Deactivated user accounts will be deleted after 90 days unless the supporting IMO has an approved exception from the IASO for the AIS. An exception must clearly state the justification for the action and the new date for account deletion. The GCCS Functional Manager is responsible to deactivate and delete GCCS JPERMS accounts IAW the regulation and CJCSM 3122.05 CONOPS for JOPES – ADP.

j. Changing Passwords: There shall be a maximum lifetime for all passwords. To protect against potential threats, it is required that a password be changed every 150 days at a minimum. For those users with domain privileges (i.e., SAs) and SIPRNET, GCCS account holders, passwords must be changed every 90 days. The maximum lifetime of a GCCS JPERMS generated password is 84 days. The minimum password lifetime is 14 days to ensure a user does not change his or her password three times in a short period of time (i.e., a few minutes, hours, and several days).

k. Expired Password: A password will be invalidated at the end of its maximum lifetime. The system will provide advanced user warning and notification that expiration of your password is approaching in order to assist in choosing a good password. The notification window begins 14 days before the expiration of password and will provide warning each login time until expiration date. If the password is not changed before the end of its maximum lifetime, the system will "lock" the user ID with the expired password. No login shall be permitted to a locked user ID until the SA/IASO unlocks it. Users must call the FCCS Help Desk to unlock their system. Then follow the same rules that apply to the initial password entry to regain access to the FCCS network.

l. Change Authorization: Consistent with the password privacy goal, users other than the SAs or IASOs, shall be permitted to change only their own passwords. To ensure compliance, users are required to enter their old password as part of the password change procedure.

m. Login to a Connected System: Users shall be required to authenticate at login with their user ID along with their password. Domain logins to the system, such as "administrator" logins, shall not be directly accessed in order for system login to be effective. Instead, system users must use their own uniquely identifiable account, and if required to perform their job function, enabling super-user equivalence using commands like "su" or "run as". It is recommended that some form of trusted identification forwarding be used between hosts when users connect to other AIS in the network. When trusted identification forwarding is not used, a remote host shall require the user's ID and password when logging in through a network connection. Administrators will have two accounts: (1) a user account for daily operations and (2) a unique administrative account for accomplishing SA tasks.

n. Remembering Passwords: It is recommended that users memorize their passwords and not write them on any medium. If passwords must be written, they shall be protected in a manner consistent with the damage that could be caused by their compromise. A suggested method is to write the password and seal it in an envelope with the seal signed by the user selecting the password. The ONLY authorized storage location of written passwords relating to the FCCS is a GSA approved classified storage facility, such as a safe – regardless of classification of the password. Locking file systems or desks WILL NOT be used to store passwords.

o. Locked Out of System: The system will lock out and prohibit the user from logging onto his/her account after three failed attempts. This is a security measure to prohibit unauthorized access to a user's account. If a user account is locked, he/she may contact the FCCS Help Desk to request the account to be unlocked. He/She will be required to verify and authenticate their identity before the SA resets the account.

p. Password Validation and Audit: The IANM shall ensure compliance with password security requirements at least every six (6) months. Password integrity shall be verified through the use of password checking routines and/or scanners.

q. Security Breach:

(1) Nullifying Exposure: Local users or their requesting IMO must pick up the password generated by the IASO in person, after presenting proper identification. Remote users must pick up their login and IASO-generated password from their local IASO. The FORSCOM IASO will forward the login and password to the remote organization IASO via FAX or secure voice. FAX transmission will only be used after voice confirmation that the IASO is standing by the FAX machine to receive the password. Remote organization IASO's must have current, official appointment orders on file at the FORSCOM IASO office. The system will require users with expired passwords to change their password before being granted access to the system.

(2) Individual Accountability: It will be considered a security violation when two or more people know the password for a SA/IASO configurable user ID, except in the case when the SA/IASO is the other person, and the user ID is identified by the system as having a newly created account or an expired password. Individual accountability and audit-ability are critical system security components.

2-3. Permissible Use of Federal Government Communications Resources.

a. Use of federal communication resources (including government-owned and leased telephones, facsimile machines, computers, e-mail, and other access to the Internet) "shall be for official use and authorized purposes only" per JER, paragraph 2-301. Authorized purposes may include personal use as permitted by "Agency Designees" within specified parameters.

b. The following personal communications are permitted: Those communications that are most reasonably made from your normal work place, such as checking in with spouse or children; making medical, home and automobile repair, and similar appointments; or making a bank or other financial transactions.

c. In order to ensure that such uses do not adversely affect the performance of official duties, this permission is subject to the following:

(1) Whenever possible, make communications before or after your work hours or during lunch or other authorized breaks.

(2) If users make them during their normal work hours, keep the communications infrequent and short.

(3) Because of the impact on the FCCS's Internet bandwidth, users may not use web-based music, television, or radio station sites for audio or visual entertainment.

(4) Users may not incur any long distance tolls or other usage fees chargeable to the government. Users must use toll-free numbers or charge the communications/access or other fees to their personal credit card.

(5) This permission does not extend to personal communications to solicit business, advertise or engage in other selling activities in support of private business enterprises, fund-raising activities (other than those permitted by JER, paragraph 3-210), accessing pornography, nor any other use that would reflect adversely on the Army or which is incompatible with public service.

(6) Users may not send group electronic mailings to offer items for sale or other personal purposes (e.g., selling an automobile or renting a private residence). Users may not send group electronic mailings to announce events sponsored by a non-federal entity without the prior approval of their supervisor.

d. The Internet provides a tremendous resource for information interchange and other communications through vehicles such as mail list servers, databases, files, and web sites. Subject to the restrictions in paragraph 2-3.c. (1 through 6) above, users must have permission to use their computers to access and use these Internet resources for:

(1) Professional development purposes, subject to the requirement that your primary duties and mission take precedence, and

(2) Any other personal reason, such as routine e-mail correspondence with your children away at college or reading a business magazine website, but only before and after work hours, or during your lunch period, or other authorized breaks during the workday.

e. In appropriate cases, your supervisor may also authorize users to use e-mail and other Internet access in support of their personal and private participation in non-federal and not-for-profit professional organizations that are subject to the limitations in paragraph 2-3.c.(5) above (See JER 3-211, paragraphs 3-300b and 3-305).

f. Users should be aware that any use of government communications resources is with the understanding that such use is generally not secure, not anonymous, and serves as consent to monitoring.

g. These policies are applicable to all military and civilian employees assigned or attached to this headquarters. They also apply to all contractors and contract employees. Violations of the policies established in this memorandum may result in criminal prosecution under Federal law, prosecution under the Uniform Code of Military Justice, adverse administrative actions, or other actions provided for in the contract.

2-4. Wireless Security.

a. Wireless devices, services and technologies which are integrated or connected to the FCCS network are considered part of the network and must comply with all FORSCOM policies and be certified and accredited.

b. Encryption of unclassified data for transmission to and from wireless devices is required. Exceptions may be granted on a case-by-case basis as determined by the DAA. At a minimum, data encryption must be implemented end-to-end over an assured channel and shall be validated under the Cryptographic Module Validation Program as meeting requirements for Federal Information Processing Standards (FIPS) Publication (Pub) 140-2, overall Level 1 or Level 2.

c. Portable Electronic Devices (PEDs) containing wireless (communications or connectivity) and/or audio/video (recording or transmission) capabilities will require specific exception by the DAA to be carried into areas where classified information is discussed or electronically processed. If approval is granted, the wireless and audio/video capabilities must be disabled while in the facility.

(1) The PEDs will support public key infrastructure, digital certificates, FIPS or National Security Agency validated crypto modules or data encryption standards appropriate for the classification level of the information processed.

(2) The PEDs must not connect to a wired and wireless network at the same time. This includes Personal Digital Assistants connected to a host computer with a synch cable.

(3) Anti-virus software will be installed, updated and used on all PEDs.

(4) All PED users must complete security awareness training regarding the physical and information security vulnerabilities and policies of the device.

(5) No PEDs, regardless of government or private ownership, or wireless/non-wireless capability will be permitted within any FORSCOM permanent, temporary or mobile Special Classified Intelligence Facility (SCIF) or Special Access Program Facilities (SAPF) without prior written approval of the cognizant Senior Intelligence Officer (SIO) or Special Access Program Security Manager, respectively. If approval is granted, transmit (radio frequency and infrared) and audio/video capabilities must be rendered completely inoperable. All PEDs will be declared to the SIO or SAP Security Manager, respectively, before entry into a SCIF or SAPF.

(6) Privately-owned PEDs will not be used to send, receive, store, process, or transmit information considered For Official Use Only (FOUO) and are not allowed to connect to DOD/FORSCOM systems. Exceptions may be granted on a case-by-case basis as determined by the DAA.

(7) The Blackberry PEDs on the Army-Approved Two-Way Wireless E-mail Devices List have the capability to send and receive data. These PEDs will be equipped with the Common Access Card sled and the Secure/Multi-purpose Internet Mail Extension software to allow digitally signed and encrypted messages. All Blackberry devices must have a password of at least five (5) characters with a minimum of one (1) alpha and one (1) numeric.

d. Wireless Local Area Networks (WLANs) are extensions of the wired FCCS network and must meet the same certification and accreditation security requirements as a wired local area network (LAN) information system.

(1) All WLANs must be engineered to preclude backdoors.

(2) All wireless data communications between a PED and the FORSCOM LAN will be secured with an appropriate FIPS Pub 140-2 encryption algorithm. This requirement can be met by using an approved Virtual Private Network (VPN) solution between the PED and FCCS network.

e. Bluetooth Personal Area Network devices have a nominal range of up to ten meters and normally use encryption. These devices are most often used to connect PEDs to peripheral devices.

(1) Bluetooth devices (including printers, PDAs, etc.) which do not support FIPS Pub 140-2 certified encryption will have the Bluetooth disabled.

(2) Bluetooth must be disabled in areas where classified information is discussed or electronically processed.

(3) Devices may not be used to process or hold official data with non-encrypted Bluetooth enabled.

2-5. Laptop Computer Use.

a. Laptops are portable desktop workstations. They are subject to the provisions of the FCCS policy on desktop workstations unless this policy specifically states an exception.

b. Only US government-owned laptop computers shall be provided connectivity to the FCCS automated information systems infrastructure.

c. The IAVA patches and windows updates are required to be installed.

(1) A FCCS server will automatically push IAVA patches and updates to the laptops used primarily as the user's desktop workstation.

(2) Laptops, not used as a workstation (stored away and used only for travel), are required to be scanned monthly to ensure IAVA patches and windows updates are installed. Prior to and upon return from temporary duty, the laptop should be scanned and certified for IAVA compliance and updates.

d. Each laptop that requires remote connection to the FCCS network will be connected via an approved VPN, or dial-in access via terminal server access control system or remote access server.

e. To ensure Command and Control compliance, laptops shall be configured by the FCCS Help Desk or the users' IMO. The current security baseline configurations for laptops operating systems are developed and maintained by RCERT.

f. Changes to the configuration baseline of laptops shall be IAW the FCCS Configuration Management Plan (CMP). Changes must be coordinated and/or approved by the FCCS Configuration Control Board (CCB).

g. Physical Security of Laptops. Whenever possible, laptop computers will be maintained under the direct supervision of the user. Users should exercise extra precautionary security measures when laptops are taken from the workplace.

(1) The computer must never be left unattended in public locations such as airports and hotel lobbies.

(2) When the computer must be left unattended, it must be stored inconspicuously (i.e., do not leave the computer sitting on the seat of an unattended vehicle).

(3) Wherever practical, the computer shall be secured with a supplied security device(s).

(4) Laptop computers will not be removed from FORSCOM premises without a DA Form 1818, Individual Property Pass, and written authorization from the users' Branch, Division or Directorate Chief. Users will not modify laptop computer equipment in any manner.

h. Users must submit a memorandum to Chief, Command and Control Support Division in order to obtain approval to configure and operate classified laptop computers on the FCCS SIPRNET and the GCCS. Requests must include the intended user, the mission requirement, and whether or not the requirement is for SIPRNET connectivity only or SIPRNET connectivity and GCCS.

2-6. Vulnerability Management.

a. Vulnerability Management is the process of finding, evaluating and remediating vulnerabilities (i.e. existing exploitable weaknesses) on servers, workstations and devices. Vulnerability management is more than Information Assurance Vulnerability Management (IAVM). It is a complete and thorough assessment of the entire system or network and the subsequent remediation efforts to correct or mitigate any deficiencies before exploitations are possible or widely publicized, in conjunction with established security mechanisms and procedures in place that add protection to the network.

b. The IAVM compliance scanning is the absolute minimum standard for all Information Systems (IS), not the preferred end-state. The IAVM does not always address IS vulnerabilities or services that pose a significant risk to the IS or network.

(1) The IAVM compliance and verification are accomplished by the FCCS SA/Network Administrator using the security test and analyst tool (STAT) Scanner, IAVA Edition in conjunction with the IAVA.dat file, which contains vulnerability checks associated with the three types of IAVM messages: information assurance vulnerability alerts (IAVAs), information assurance vulnerability bulletins (IAVBs), and information assurance technical tips (IATTs).

(2) The IAVM requires the completion of four distinct phases to ensure compliance. These phases are:

(a) Vulnerability identification, dissemination, and positive acknowledgement.

(b) Application of measures to affected systems to make them compliant.

(c) Compliance reporting.

(d) Compliance verification.

c. The Network Enterprise has an approved IA assessment tools list that is authorized on the Blanket Purchase Agreement through the Communications Security Logistics Agency.

d. The SAs, IANMs and IASOs must be Level II certified in addition to any certification training requirements as appropriate for FCCS network configuration.

e. Appendix C, Scanning Requirements, is an extract of scanning requirements from AR 25-2 and the memorandum, DA CIO/G-6, (NETC-EST-IAD), 7 July 2004, subject: Implementation of Information Assurance Best Business Practice, 04-EC-0-0004: Network Assessment Scanning; Version 1.0.

2-7. Hardware, Software and Removable Media Security.

a. Labels should be displayed on all components of an IS. This includes input/output devices that have the potential for retaining information, terminals, stand-alone microprocessors and word processors used as terminals. Each device should bear conspicuous external labels stating the highest classification level and most restrictive classification category of the information accessible to the components in the IS.

b. Low risk software must be approved by the FCCS DAA before use on the FCCS networks. Low risk software is:

(1) Provided officially by another US Government Agency that has equivalent standards.

(2) Developed within a Government-approved facility.

(3) Commercial-off-the-shelf software provided through appropriate procurement channels.

(4) Distributed through official channels.

(5) Acquired from a reputable vendor for official use or evaluation.

c. Certain software is deemed “high risk” and is not authorized for use without approval. High risk software includes public domain, demonstration software, and embedded software not obtained through official channels. The FCCS must approve such software in writing before it may be legally used.

(1) Floppy diskettes and removable media used for demonstrations, with intent of being returned to the vendor, must be processed on a computer that has never processed or stored classified data. Vendor hardware used for software demonstrations must operate in a stand-alone mode. Approval from the FCCS DAA must be obtained before use of vendor software for demonstration purposes on the FCCS network.

(2) Types of unauthorized software include:

(a) Public domain software or “shareware” which have been obtained from unofficial channels.

(b) Personally owned software (either purchased or gratuitously acquired).

(c) Software from unknown sources.

(d) Illegally copied software in violation of copyright rules.

(e) Music and video or multimedia compact disks not procured through official Government channels.

d. Removable IS storage media and devices shall have external labels clearly indicating the classification of the information and applicable associated markings. Examples include magnetic tape reels, cartridges, cassettes, removable discs, disc cartridges, disc packs, diskettes, magnetic cards, universal serial bus "thumb" memory devices and electro-optical media.

(1) Labels will be affixed to all media in a manner that does not adversely affect operation procedures.

(2) Labels for compact disks (CDs) must not be placed on the CD itself. Place the labels on the CD container or envelope.

2-8. Classified Spillage and Reporting Responsibilities.

a. A classified spillage incident is defined as an occurrence where classified information is transmitted, received, or processed on a computer system/network not authorized for the processing of that level of classified information. An example would be a Confidential or Secret document sent via e-mail over the unclassified network.

b. All employees, users, supervisors, and Directorate/Division/Branch IASOs and Security Managers must follow the procedures at Appendix D, Spillage Reporting Responsibilities, when a classified spillage incident occurrence has been recognized. Each step of the procedures must be completed before the classified spillage incident can be considered closed and the network returned to its original classification.

2-9. Virtual Private Network Security.

a. There is an immediate demand for secure high-speed access to Army installations from authorized telecommuters, travelers and other remote users. The Terminal Server Access Controller System (TSACS) provides remote access for users. However, TSACS is a dial-up technology using the public switch telephone network and is low speed by today's standards. The remote access server is a mechanism for dial-up to complement the TSACS. A VPN is the preferred technology to provide secure high-speed remote access to the FCCS NIPRNET and other Wide Area Networks.

b. A VPN is a way to use public Internet to provide remote offices or individual users with secure access to their organization's network.

c. The following are requirements for VPN secure remote client access:

(1) All computers used to access VPN shall be government furnished equipment.

(2) All VPN systems shall meet the certification and accreditation requirements of AR 25-2, Information Assurance, 23 Nov 03.

(3) Remote access shall use approved encryption to protect the confidentially of the session. The Advanced Encryption Standard 128 (128 bit Advanced Encryption Standard) or higher is the preferred encryption standard.

(4) All decrypted VPN traffic shall be visible by either an approved host or network based Intrusion Detection System/Intrusion Protection System (IDS/IPS), configured to provide centralized audit server support and management.

(5) All ISs that use a VPN to connect to the FCCS NIPRNET through dial-up, digital subscriber line, integrated services digital network, cable modem, or similar connections shall have an approved firewall installed on the VPN host and an approved anti-virus software application installed and continuously enabled and updated.

(6) Split-tunneling of VPN connections is prohibited. Split-tunneling allows the VPN client to use both the encrypted tunnel to the installation and the same high-speed connection for unencrypted traffic to the Internet. Split-tunneling is vulnerable for computer compromise and opens up an avenue of attack from the unencrypted traffic through the encrypted tunnel.

2-10. Firewall.

a. The firewall system will restrict access to and from the FCCS network such that the risk of unauthorized penetration and data transfer through the network is minimized with only authenticated and/or authorized services being specifically allowed to pass through the firewall components. A firewall system is comprised of firewalls, proxy servers, VPN concentrator, IDS/IPS, and access control lists on connectivity nodes. Using a standard set of components (to the maximum extent possible), each firewall will be tailored and configured to support the specific network connectivity requirements of the particular domain, enclave, site, or functional group.

b. Firewalls employed on the FCCS network must meet the following general requirements:

(1) All firewalls deployed on the FCCS network will be on the approved Communications Security Logistics Activity IA Tools List.

(2) Factory Shipped Configuration: Firewalls must be configured by default to deny all services when shipped.

c. The Physical Security aspect of the firewall will ensure that:

(1) The firewall hardware is located in a controlled environment with unescorted access to the IAM/IANM, the firewall administrator and their alternates.

(2) Anyone entering the firewall enclosure without unescorted access privileges shall sign a visitor's log before entering and upon leaving the firewall area.

(3) The firewall enclosure shall be equipped with heating, air conditioning and smoke alarms to assure a proper operating environment for electronic equipment.

(4) The firewall shall be protected against unauthorized hardware or software modifications by establishing an event/change modification log.

d. Firewall Administrative Security:

(1) The firewall administrator and the alternate shall be trained in administration, operation and maintenance of the firewall.

(2) The firewall administrators shall be designated as Information Technology-I positions and have the appropriate background investigations completed as specified in AR 380-67 and AR 25-2.

(3) The firewall shall be accredited IAW DODI 5100.4, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), after installation. Re-accreditation shall be IAW AR 25-2, chapter 5, paragraph 5-5.

(4) Systems that are to be protected by the firewall shall be explicitly identified.

(5) Deliberate violations of this firewall policy document shall be subject to appropriate disciplinary action based on the severity of the violation.

(6) Firewall password assignment and distribution are performed as follows:

(a) The firewall administrator or IANM/IAM will assign passwords.

(b) The IANM/IAM or designated IASO will distribute passwords.

e. Firewall Configuration:

(1) The firewall must be located and configured so that it can control all communications between the protected network and the systems on the outside of the firewall.

(2) All dial-in or dial-out modem connections on the protected network must go through the firewall.

(3) A second firewall (if applicable) will be configured as a failover due to problems (e.g. downtime, performance, etc.) directly related to the primary firewall.

(4) The firewall must be configured to withstand deliberate denial-of-service attacks such as "SYN flooding" or "ping of death" attacks.

(5) Direct/indirect logins shall be used for the firewall. Direct/indirect login privileges shall be restricted to the IANM, firewall administrator, and their alternates.

(6) Only the firewall administrator or alternate administrator will do any modifications of the firewall software unless authorization is given from appropriate supervisor and noted in the event/change modification log.

(7) The firewall shall require authentication before permitting a process to pass through to the protected network.

(8) The firewall shall be configured to be capable of establishing a VPN with another site and passing encrypted information.

(9) The firewall shall be configured to be capable of detecting, prohibiting and reporting a hacker's attempt to do port scanning.

(10) The firewall may not contain any compilers, editors, communications software, user applications, or any other files other than those directly related to the functioning of the firewall.

(11) The firewall shall report or log all violations of this policy.

(12) Only the IAM/IANM, the firewall administrator or their alternates shall maintain the audit trail or logs on files accessible.

(13) The firewall audit trail or event logs shall be maintained on file for a period of 180 days.

(14) Alarm and alert functions on the firewall and any other perimeter access control devices shall be enabled.

(15) In the event of a reportable incident, see the incident response reporting procedures contained in the IA Incident Detection and Response Plan.

(16) Vulnerability scans should be conducted at least quarterly as part of routine maintenance.

(17) Application level firewalls shall not be configured so that outbound network traffic appears as if the traffic had originated from the firewall, i.e., internal addresses are hidden from the outside networks.

(18) All inbound Internet services must be processed by proxy software on the firewall. If a new service is requested, it shall not be made available until a proxy is available on the firewall.

(19) The firewall's system integrity database shall be updated each time the firewall's configuration is modified. System integrity files shall be stored on read-only media or on off-line storage media.

(20) The firewall should fail to a configuration that denies all services, and require the firewall administrator to re-enable services after a failure.

(21) Source routing shall be disabled on the firewall.

(22) The firewall shall alarm the firewall administrator of any item that may need immediate attention so action can be taken.

f. Firewall Protocol Access: The following describes the type of protocols that will and will not have access into and out of the firewall:

(1) Hypertext Transport Protocol (HTTP): The HTTP will not be blocked from inside (trusted) network. Protocols will be blocked from outside (un-trusted) the network by destination Internet Protocol (IP) and destination host name.

(2) File Transfer Protocol (FTP): Outbound/inbound FTP traffic will not be allowed through the firewall from IP addresses or host name without the use of encryption.

(3) Telecommunications Network (TELNET): TELNET will not be permitted to pass outbound/inbound traffic through the firewall without the use of encryption.

(4) Simple Mail Transfer Protocol (SMTP): SMTP will be permitted through the firewall but only to the mail server on the trusted side.

(5) Post Office Protocol 3 (POP3): POP3 traffic will not be permitted to pass through the firewall without the use of encryption.

2-11. Intrusion Detection System/Intrusion Protection System.

a. The IDS/IPS will monitor access to the FCCS network such that the risk of unauthorized activity will trigger alerts. Using a standard set of components (to the maximum extent possible), each IDS/IPS will be tailored and configured to support the specific network connectivity requirements of the particular domain, enclave, site, or functional group.

b. All IDS/IPSs deployed on the FCCS network must be on the Department of Army Chief Information Officer (CIO) G-6 Recommended IA Automated Tools List.

c. The physical security aspect of the IDS/IPS will ensure that:

(1) The IDS/IPS hardware is located in a controlled environment with unescorted access to the IAM/IANM, the IDS/IPS administrator and alternates.

(2) Anyone entering the IDS/IPS enclosure without unescorted access privileges shall sign a visitor's log before entering and upon leaving the IDS/IPS.

(3) The IDS/IPS enclosure shall be equipped with heating, air conditioning and smoke alarms to assure a proper operating environment for electronic equipment.

d. IDS/IPS Administrative Security:

(1) The IDS/IPS administrator and the alternate are to be trained in the administration, operation and maintenance of the IDS/IPS.

(2) The IDS/IPS administrators are designated as Information Technology-II positions. Appropriate background investigations shall be completed as specified in AR 380-67 and AR 25-2.

(3) The IDS/IPS will be accredited IAW the DITSCAP after installation. Re-accreditation will be IAW AR 25-2, Chapter 5, paragraph 5-5.

(4) Systems shall be explicitly identified where IDS/IPS is used for monitoring.

(5) Deliberate violations of this IDS/IPS policy document will be subject to appropriate disciplinary action based on the severity of the violation.

e. IDS/IPS password assignment and distribution are performed as follows:

(1) The IDS/IPS administrator or IANM will assign passwords.

(2) The IANM or designated IASO will distribute passwords.

f. IDS/IPS Configuration:

(1) The IDS/IPS must be located and configured so that it can monitor all communications between the firewall and protected network.

(2) All dial-in or dial-out modem connections on the protected network must go through the IDS/IPS.

(3) Only the IDS/IPS administrator or alternate administrator will do any modifications of the IDS/IPS software unless authorization is given from appropriate supervisor and noted in the event/change modification log.

(4) The IDS/IPS shall be configured to monitor, detect and report a hacking attempt.

(5) The IDS/IPS audit trail or event logs shall be maintained on file for a period of 180 days.

(6) Alarm and alert functions on the IDS/IPS and any other perimeter access control devices shall be enabled.

(7) In the event of a reportable incident, see the incident response reporting procedures contained in the Information Assurance Incident Detection and Response Plan.

(8) Vulnerability scans should be conducted at least quarterly as part of routine maintenance.

(9) The IDS/IPS shall alarm the IDS/IPS administrator in near real-time of any item that may need immediate attention so that immediate action is taken.

2-12. Servers.

a. There must be an explicit and well-defined security policy enforced for each operating platform. For network servers:

(1) All guest accounts shall be disabled.

(2) Administrator accounts shall be renamed if the system makes provision for it.

(3) Accounts shall be locked after three unsuccessful attempts within a 30-minute period and the SA and IASO are notified.

(4) Only SAs shall unlock accounts.

(5) Audit records shall be generated to document when account lockouts occur.

(6) Remote administration of servers over the NIPRNET, Internet, etc., shall be accomplished via a secure communications path (e.g., VPN, etc.).

b. Accountability: Audit information shall be retained and protected so that actions affecting security can be traced to the responsible party. Each network server shall be scanned at least twice a year using approved security scanning software. The purpose of server audits is to confirm the degree to which actual configurations are reflected in baseline configuration files. Further, they verify the degree to which changes in server configuration have been documented and approved in the configuration management processes.

c. Baseline:

(1) All servers shall be loaded and configured with a standard baseline image that is consistent with the most recently Army Computer Emergency Response Team (ACERT) approved security patches and fixes. The current Army security baseline configurations for server operating systems are developed and maintained by ACERT and can be found at https://iassure.army.mil/security. Microsoft product baselines can be found at https://iassure.army.mil/security/microsoft.

(2) Only servers with built-in auditing and logging capability shall be deployed.

(3) Servers shall be configured to utilize built-in auditing capabilities IAW the current governing policy on operational controls.

(4) Servers shall have the capability to allow discretionary access control to the directory and file level.

d. Documentation: A baseline of all server documentation shall be maintained by the SA. This documentation shall include, but is not limited to, Standard Operating Procedures, Server System Administration Guides, Server Deployment Guides, and Server Change Management documents. Documentation shall reflect updates as server configurations and baseline changes are implemented.

e. Continuous Protection:

(1) The "trusted" mechanisms that enforce these basic requirements shall be continuously protected against tampering and/or unauthorized changes. Attempts to modify the system services, whether successful or not, shall be recorded in security logs. This provides a documented record of all user and system changes attempted and made.

(2) Security, application, and system audit logs shall be copied nightly. Systems shall be backed up on a regular basis and backups stored in a secure off-site location.

f. Physical Security Policy: Servers shall be located in secured facilities with controlled access.

g. Documentation and Configuration Management:

(1) Maintenance of up-to-date configuration documentation and configuration management records is the responsibility of the SA.

(2) Server configuration documentation shall be retained by the SA and audited annually by the IAPM or designee IAM to ensure that proper configuration management controls are being used.

(3) The SA or IASO shall review server level security logs on a daily basis at a minimum. The SA or IASO shall take immediate action to resolve security events detected through the review of security logs. Once the log is reviewed and unexplained security events resolved, it shall be validated for retention or destruction IAW log retention policies.

(4) Changes to the configuration baseline shall be IAW with the FCCS CMP and coordinated and/or approved by the FCCS CCB.

2-13. Routers/Switches.

a. Only US Army approved network protocols shall be used on FCCS networks.

b. No other protocols are officially supported or allowed on the FCCS networks. It is understood that certain network protocols are inherently required for certain computer systems, but they are typically limited to a single segment and do not cross router boundaries.

c. The TELNET access (for remote administration) shall be restricted to specifically identified “internal” workstations only by applying "vty" port access lists.

d. Simple Network Management Protocol community names with “read-write” strings shall be configured with unique names (i.e., names other than “private”).

e. Any default community names shall be configured to have “read only” permissions.

f. Security checks shall be performed on all routers. The security logs shall be collected in a central location for review and analysis by the IA staff.

g. In order to improve security, the FCCS router engineers and system administrators shall make the following changes to generic CISCO router configuration:

(1) Enable the “No IP source-route.” This configuration prevents source-routed packets which can be used to circumvent security measures.

(2) Provide routers connected to external networks with access lists that deny remote access to ports 135-139 on both transmission control protocol (TCP) and user datagram protocol (UDP). These ports are used by Network Basic Input Output System and can be used to compromise security on MS Windows servers.

(3) Router access lists shall be installed that deny incoming packets with source addresses equal to the internal network. This will prevent “spoof” attacks from external unauthorized users.

(4) The following router command lines are standard and will be employed: "No TCP-small-servers" and "No UDP-small-servers". These router command lines disable the normal set of diagnostic processes found on routers and most UNIX platforms. They can be used to initiate "denial of service" attacks.

(5) Remove the "enable password." Retain only the "enable secret" password, which is encrypted before saving.

(6) After modifying router configurations, save the change to the startup configuration as well as to any back-up location designated, such as a trivial file transfer protocol server.

h. Router Documentation: The configuration of each router shall be documented in a baseline documentation file. Only material changes to router configurations shall be submitted to the CCB and documented in a CMP. Emergency changes may be made with the verbal approval of the IAM, IANM or IAPM as operationally required. However, at the earliest opportunity, a change request must be submitted to the CCB and, when approved, the change posted in the router baseline documentation and in the CMP.

i. The IANM or designee shall audit each network router at least twice a year. The purpose of router audits is to confirm the degree to which actual configurations are reflected in router baseline configuration files. Further, they verify the degree to which changes in router configuration have been documented and were approved in the configuration management processes.

j. Router administrators are accountable for ensuring that router documentation and change management records are up-to-date. They are responsible for correcting documentation for any routers found to be out of compliance with the above policies.

k. Changes to the configuration baseline shall be IAW the FCCS CMP and coordinated and/or approved by the FCCS CCB.

l. The network shall be configured so communications from non-protected internal tenants addressed to tenants in a protected area shall be routed through a firewall. There shall be no data communication paths allowed that route data communications to and from protected resources without going through a firewall.

m. Web hosts located in a demilitarized zone (DMZ) shall be accessible from within the protected area of the network through a router and firewall configured to allow only outbound communications.

n. Web hosts located in the DMZ shall be accessible by the public, and internal resources not located in a protected area of the network, through a router that forces the communication through a firewall configured to allow only required services (e.g., http, smtp, etc.).

o. Router access control lists shall be used to further restrict access to selected network objects based upon user requirements.

APPENDIX A - Acceptable Use Policy (User)

Acceptable Use Policy

1. Understanding: I understand that I have the primary responsibility to safeguard the information contained in the Forces Command (FORSCOM) Command and Control System (FCCS) Secret Internet Protocol Router Network (SIPRNET), FCCS Nonclassified Internet Protocol Router Network (NIPRNET) and the Global Command and Control System (GCCS) from unauthorized or inadvertent modification, disclosure, destruction, denial of service and use.

2. Access: Access to these networks is for official use and authorized purposes and as set forth in Department of Defense (DOD) 5500.7-R, "Joint Ethics Regulation" or as further limited by this policy.

3. Revocability: Access to Army resources is a revocable privilege and is subject to content monitoring and security testing.

4. Classified information processing: The FCCS SIPRNET is the primary classified information system for FORSCOM. The FCCS is a United States (US) only system and approved to process classified collateral information.

a. The FCCS SIPRNET provides classified communication to external DOD and other US Government organizations using the SIPRNET. Primarily this is done via electronic mail (e-mail) and Internet networking protocols such as web, file transfer protocol (FTP) and telecommunications network (TELNET).

b. The FCCS SIPRNET is authorized for SECRET or lower level processing in accordance with the FCCS System Security Authorization Agreement. It can also process UNCLASSIFIED, SENSITIVE information in accordance with AR 25-2.

c. The classification boundary between FCCS SIPRNET and FCCS NIPRNET requires vigilance and attention by all users. The FCCS SIPRNET is a US only system and not accredited for transmission of North Atlantic Treaty Organization material.

d. The ultimate responsibility for ensuring the protection of information lies with the user. The release of TOP SECRET information through the SIPRNET is a security violation and will be investigated and handled as a security violation or as a criminal offense.

e. The GCCS resides on the FCCS SIPRNET. It is classified SECRET and provides information for the warfighter to plan, execute and manage military operations. The FORSCOM GCCS Functional Manager issues an account and password to the user for GCCS access. The FORSCOM Joint Operation Planning and Execution System (JOPES) Functional Manager will grant access to JOPES OPLANS, for users with a valid requirement and proof of training, using JPERMS.

5. Unclassified information processing: The FCCS NIPRNET is the primary unclassified information system for FORSCOM. The FCCS is a US only system.

a. The FCCS provides unclassified communication to external DOD and other US government organizations. Primarily, this is done via e-mail and Internet networking protocols, such as web, FTP and TELNET.

b. The FCCS is approved to process UNCLASSIFIED, SENSITIVE information in accordance with AR 25-2. The release of classified information through the NIPRNET is a security violation and will be investigated and handled as a security violation or as a criminal offense.

c. The FCCS and the Internet, as viewed by FORSCOM, are synonymous. The e-mail and attachments are vulnerable to interceptions as they traverse the NIPRNET and Internet.

6. Minimum security rules and requirements: As a FCCS SIPRNET, FCCS NIPRNET, and/or GCCS system user, I will comply with the following minimum security rules and requirements below:

a. I am not permitted access to FCCS SIPRNET, FCCS NIPRNET, or GCCS unless in complete compliance with the FORSCOM personnel security requirement for operating in a SECRET system-high environment.

b. I have completed the user security awareness training module and successfully passed the test. I will participate in all training programs as required, inclusive of threat identification, physical security, acceptable use policies, malicious content and logic identification, and non-standard threats, such as social engineering, before receiving system access.

c. I will generate, store, and protect passwords or pass phrases. Passwords for the FCCS SIPRNET and FCCS NIPRNET will consist of at least ten characters with a minimum of two uppercase and lowercase letters, numbers, and special characters. Passwords for the GCCS will consist of eight characters (six alpha and two numeric). I am the only authorized user of these accounts. I will not use my user identification, common names, birthdays, phone numbers, military acronyms, call signs, or dictionary words as passwords or pass phrases.

d. I will use only authorized hardware and software. I will not install or use any personally owned hardware, software, shareware, or public domain software.

e. I will use virus checking procedures before uploading or accessing information from any system, diskette, attachment, or compact disk.

f. I will not attempt to access or process data exceeding the authorized Information System (IS) classification level.

g. I will not alter, change, configure, or use operating systems or programs, except as specifically authorized.

h. I will not introduce executable code, such as, but not limited to, .exe, .com, .vbs, or .bat files, without authorization, nor will I write malicious codes.

i. I will safeguard and mark, with the appropriate classification level, all information created, copied, stored, or disseminated from the IS and will not disseminate it to anyone without a specific need to know.

j. I will not utilize Army or DOD provided IS for commercial financial gain or illegal activities.

k. Maintenance will be performed by the System Administrator (SA) only.

l. I will use screen locks and log off the workstation when departing the area.

m. I will immediately report any suspicious output, files, shortcuts, or system problems to the FCCS SA and/or Information Assurance Security Officer (IASO) and cease all activities on the system.

n. I will address any questions regarding policy, responsibilities and duties to FORSCOM SA and/or IASO.

o. I understand that each IS is the property of the Army and is provided to me for official and authorized use only. I further understand that each IS is subject to monitoring for security purposes and ensuring use is authorized. I understand that I do not have a recognized expectation of privacy in official data on the IS and may have only a limited expectation of privacy in personal data on the IS. I realize that I should not store data on the IS that I do not want others to see.

p. I understand that monitoring of FCCS will be conducted for various purposes. Information captured during monitoring may be used for administrative or disciplinary actions and/or for criminal prosecution.

(1) I understand that the following activities define unacceptable uses of an Army IS:

(a) Anything that would reflect adversely on the Army is prohibited use on the network.

(b) The DOD 5500.7-R, Joint Ethics Regulation, defines spam, profanity, sexual content, and gaming as unethical. These are prohibited activities on the FCCS.

(c) Prohibited sites or activities are pornography, obscene material (adult or child), copyright infringement, transmission of chain letters, unofficial advertising, soliciting, selling (except on authorized bulletin boards established for such use), or the violation of any statue or regulation.

(2) I understand that the following activities define acceptable use of an Army IS:

(a) Communications that are most reasonably made from your normal work station (such as, but not limited to, brief Internet searches, e-mail to check in with spouse or children, schedule medical, home and automobile repair and similar appointments or make a bank or other financial transaction) are permitted. When possible, make communications before or after work hours or during lunch or other authorized breaks.

(b) I may have permission to use a computer to access and use Internet resources for professional development purposes and other personal use such as reading a business magazine website. However, I am to do so only before or after normal work hours or during authorized breaks.

(c) In appropriate cases, my supervisor may also authorize the use of e-mail and other Internet access in support of personal and private participation in non-federal and non-profit professional organizations. However, this is subject to limitations as stated above.

q. Violation of this policy may result in criminal prosecution under Federal law, prosecution under the Uniform Code of Military Justice, adverse administrative action or other actions provided for in contract. (NOTE: Prohibited activities found on my computer can lead to criminal offenses.)

r. The information below will be used to identify users and may be disclosed to law enforcement authorities for investigating or prosecuting violations. Disclosure of this information is voluntary; however, failure to disclose information could result in denial of access to the FCCS SIPRNET, FCCS NIPRNET and GCCS information system.

7. Acknowledgement: I have read the above requirements regarding use of FCCS and GCCS information systems. I understand my responsibilities regarding these systems and the information contained in them.

_____	_____
Directorate/Division/Branch	Date
_____	_____
Last Name, First, MI	Rank/Grade
_____	_____
Signature	Phone Number

APPENDIX B - System Administrator Acceptable Use Policy

AFCI-IC

MEMORANDUM FOR Chiefs, Primary and Special Staff Agencies

SUBJECT: System Administrator (SA) Acceptable Use Policy for Forces Command (FORSCOM) Command and Control System (FCCS)*

1. References:

a. Army Regulation 25-2, Information Assurance, 14 November 2003.

b. Army Regulation 25-1, Army Knowledge Management and Information Technology Management, 30 June 2004.

2. It is the responsibility of the FORSCOM Deputy Chief of Staff, G-6, Command and Control Support Division to provide operational and maintenance support for all components of the FCCS. To ensure reliability, availability, and supportability of all systems and data on the FCCS internal network, the following guidelines are issued with regard to SA and user rights for FCCS components.

3. By definition, user rights are rules that determine the actions a user can perform on systems supported by the Windows Platform. The SA have elevated rights and privileges allowing complete access and authority to the system to which they administer. Extreme vigilance is required when issuing administrative rights, as destruction of network resources may occur with novice or untrained users.

4. Guidelines for SA rights:

a. Domain Administrators. The SA rights with domain controller authority is limited to the G-6, Command and Control Support Division, Network Services Branch only. The Domain Administrator account password will be tightly controlled and issued by signature only from the Information Assurance Security Officer (IASO). The Command and Control Support Division, Network Services Branch Chief must approve access to this account.

b. Local Administrators. Members of a server or workstation local administrators group have complete authority over the workstation on which the group resides. The SA rights for local workstations are limited to the FCCS Support Team AFCI-IC
SUBJECT: System Administrator (SA) Acceptable Use Policy for Forces Command (FORSCOM) Command and Control System (FCCS)

Support Team. Exception to this policy may be granted upon request. Exception to policy should be forwarded through the Information Management Officer channels to the Network Services Branch. The following are guidelines for exception to policy approval:

(1) Microsoft Certified Professional (MCP) certification or Level I IASO Training (online website at Fort Gordon http://ia.gordon.army.mil/iaso/) meets the minimum requirement to obtain Administrator privileges.

(2) The MCP certified personnel have demonstrated in-depth knowledge of at least one Microsoft operating system, and Level l trained personnel have acquired the basic tools used to identify security standards for Department of the Army Information Systems.

(3) Users who have obtained MCP or Level l status may be granted local administrative rights to their Windows workstation or server.

c. Developers Group. Members of the G-6 Command Data Support Branch or other such development groups may be granted local administrative rights to their workstations by following procedures for minimum requirements stated in paragraph 4b above.

5. Should the user require FCCS Support Team assistance to rebuild or return a workstation or server to operational status, the users' local administrative rights may be revoked if it is determined that failure of the Information System was due to the user negligence. Final authority for revoking user administrative rights is the Designated Approving Authority (DAA). (All exceptions granted to this policy are granted by the DAA.

6. For additional information or assistance, please contact your staff IMO or the FCCS Customer Support Center, 464-2222.

WILLIAM T. LASHER
Colonel, SC
Deputy Chief of Staff, G-6

---

*This memorandum supersedes FORSCOM Policy Memorandum 25-05-01, dated 15 February 2005

APP/ENDIX C - Scanning Requirements

Scanning Requirements			
Requirements	**Type**	**Schedule**	**What to Look For**
IAVM	FCCS network Assessment	Immediate	Identify assets that require remediation.
IAVM Mitigation Plans	FCCS network Assessment	Immediate	Validation of remediation plans and configurations.
Password Compliance	FCCS network Assessment	Monthly on a rotational schedule or as directed	Specific scanner policy to identify individual requirements. Blank administrator, and guest accounts, default or "out of the box" implementations.
Illegal Software Installation	FCCS network Assessment	Monthly on a rotational schedule or as directed	Specific scanner policy to identify individual requirements.
Required Software	FCCS network Assessment	Monthly on a rotational schedule or as directed	Specific scanner policy to identify individual requirements.
Policy Enforcement	FCCS network Assessment	Monthly on a rotational schedule or as directed	Specific scanner policy to identify individual requirements.
RAS VPN Wireless	FCCS network/DOIM Assessment	Monthly	Illegal or mis-configured connectivity, configuration, poor security, non-compliance, policy enforcement, changed requirement, etc.
IAM/IASO Enclave Assessment	DITY VAP	Quarterly	Identify application, network, and operating system vulnerabilities, configuration errors, and unauthorized access points.
TLA Infrastructure Systems and Devices	FCCS network/DOIM Assessment	Quarterly	Configuration, poor security, non-compliance, policy enforcement, changed requirements, etc.
IS	FCCS Comprehensive Vulnerability Assessment	Semi-annual	All available scanner policies. Configuration, poor security, non-compliance, policy enforcement, etc.
Networks	FCCS network Assessment	Semi-annual	CRD 100 percent asset inventory update.
Networks	FCCS network/DOIM Assessment	Semi-annual	Backdoors, illegal modems, unaccredited connections.
Network Devices	FCCS network/DOIM Assessment	Semi-annual	Legacy or non-supported networked devices presenting a possible Disk Operating System (DOS) threat.
Revalidation of SIPRNET CAP	FCCS network/DOIM Assessment	Annual	Configuration, poor security, non-compliance, policy enforcement, changed requirements, etc.
Web Sites	FCCS network/DOIM Assessment	Annual	Operation Security (OPSEC) Review. Configuration, poor security, non-compliance, policy enforcement, changed requirements, etc.

APPENDIX D - Spillage Reporting Responsibilities

1-1. USER:

a. Recognize the incident.

b. Immediately send out a request for Recall of Unread E-mails to all original addressees. Do not forget the "auto-forwarding" and "blind courtesy copy" capabilities of the system.

c. Immediately send out a notification e-mail to all addressees, send the incident e-mail, identifying the e-mail date, time, and subject line of the incident e-mail. Request that all addressees perform the following actions:

(1) Delete the incident e-mail from their e-mail Inbox.

(2) Delete the incident e-mail from their e-mail Deleted Items.

(3) Notify their servicing Director of Information Management (DOIM)/Information Technology Business Center (ITBC) Help Desk of the classified content e-mail so the DOIM/ITBC may begin the purging procedures of their e-mail servers.

(4) Determine if the addressee has forwarded the incident e-mail to additional addressees. If addressee has forwarded the incident e-mail, the addressee must perform all steps indicated here, starting at b above.

(5) Notify their Information Assurance Security Officer (IASO) and Security Manager.

(6) Addressee must inform originator when all of the above purging actions have been successfully accomplished.

d. Immediately notify the Forces Command (FORSCOM) Command and Control System (FCCS) Help Desk (404-464-2222) of the e-mail date, time, and subject line of the incident e-mail.

e. Notify the immediate supervisor, IASO, and Security Manager of the incident.

f. If the incident e-mail was printed, bring the printed document under control, properly stamp the classification on the printed document, and properly store the printed document.

g. Forward all responses received from original addressees to the immediate supervisor, IASO, and Security Manager.

h. When instructed to do so by the IASO or servicing technician from the G-6 Command and Control Support Division, delete the incident e-mail from their e-mail Inbox, delete the incident e-mail from their e-mail Sent Items, and delete the incident e-mail from their e-mail Deleted Items.

i. Be prepared to provide the Preliminary Inquiry Officer with all information available on the incident.

1-2. SUPERVISOR:

a. Verify classification of incident e-mail.

b. Verify user has sent the recall e-mail request to all original addressees.

c. Verify user has sent the Incident Notification E-mail to all original addressees of the nature of the incident and of all of the clean up procedures that must be followed to purge this incident from their local area network.

d. Verify the FCCS Help Desk has been notified of the incident.

e. Determine if the user printed the incident e-mail. If so, was it brought under control and properly stored.

f. Notify the IASO, Security Manager, and Directorate Chain of Command of the incident.

g. Forward all responses received from original addressees to the IASO and Security Manager.

h. Provide the Preliminary Inquiry Officer with all information available on the incident.

1-3. Information Assurance Security Officer (IASO):

a. Notify the FCCS Information Assurance Manager (IAM) (404-464-5444) and the FCCS Information Assurance Network Manager (IANM) (404-464-7464) of the incident.

b. Ensure the FCCS Help Desk (404-464-2222) is aware of the incident.

c. Ensure the Security Manager is aware of the incident.

d. Assist the G-6 Command and Control Support Division servicing technician in finding the user and computer system where the incident occurred.

e. Ensure the incident e-mail is deleted from the users e-mail Inbox, Sent Items, Deleted Items, all Recycle Bins and storage devices.

f. Forward all responses received from original addressees to the Security Manager and the FCCS IAM and IANM.

g. Provide the Preliminary Inquiry Officer with all information available on the incident.

1-4. Security Manager:

a. Notify the FORSCOM G-2 Security Division (404-464-7610) IAW paragraph 2-13b(1), FORSCOM Memorandum 380-5, Department of the Army Information Security Program, 15 November 2003, of the incident.

b. Notify the G-6 Security Manager (404-464-5023) of the incident.

c. Ensure the Directorate Chain of Command has been notified of the incident.

d. Ensure a Preliminary Inquiry is conducted IAW paragraph 2-13c(1), FORSCOM Memorandum 380-5, 15 November 2003, of the incident.

1-5. FCCS Help Desk:

a. Accurately log the occurrence of the incident and the e-mail date, time, and subject line of the incident e-mail.

b. Notify the FCCS IAM and IANM (404-464-5444) of the incident at the earliest possible time, during normal business hours.

1-6. FCCS IAM and FCCS IANM:

a. Task service technicians to visit each affected computer system within the network to perform a delete of the incident e-mail from the users e-mail Inbox, Sent Items, Deleted Items, all Recycle Bins and storage devices. Ensure the service technicians investigate whether the user was utilizing:

(1) Auto-Forwarding.

(2) Blind Courtesy Copy.

(3) Auto-Replies.

(4) Auto-Archive.

(5) If the user printed the incident e-mail.

b. Ascertain if the incident e-mail was transmitted to a Blackberry user.

c. Ascertain if the incident e-mail was retained on the network long enough for scheduled backup to occur. If so, ensure the backup tape is recovered, properly marked, and properly stored.

d. Schedule a maintenance defragmentation routine to be run on all affected mail/exchange servers as soon as operationally feasible.

e. Notify the G-6 Security Manager (404-464-5023) of the incident.

f. Notify the G-6 Chain of Command of the incident.

g. Be prepared to provide the Preliminary Inquiry Officer with all requested information available on the incident and all purge procedures initiated to clear the incident. If the incident e-mail was transmitted to a Blackberry user, inform the Preliminary Inquiry Officer there is no way to be assured the classified information was not compromised.